



# BUSINESS TRAVEL TIPS

**You or your firm may be a target of a foreign country's efforts to obtain information or technologies in order to increase its market share, build its economy, or modernize its military.**

**Targeting methods include luggage searches, extensive questioning, and unnecessary inspection and downloading of information from laptop computers.**

## BEFORE YOU TRAVEL

- Obtain specific pre-travel country risk assessments
- Clear personal data or information from your computer, smart phone or other digital device. If you don't need the device, don't take it.
- Make copies of your passport, airplane ticket, driver's license, and credit cards that you take with you. Leave one copy at home
- Establish points of contact for emergencies
- Register your trip with the State Department
- Obtain the phone number and address for the U.S. Embassy or Consulate in the country(s) you plan to visit
- Clean out your voice mail
- Familiarize yourself with local laws and customs in the areas you plan to travel
- Plan your wardrobe so that it does not offend local residents, or draw unwanted attention to yourself
- Do not take unnecessary identification or credit cards

## DURING YOUR STAY

- Protect your passport!
- Use authorized taxis
- Do not invite strangers in your room
- Do not carry large amounts of cash
- Do not leave drinks unattended
- Avoid long waits in lobbies and terminals
- Be aware of new acquaintances who probe for information
- Avoid civil disturbances and obey local laws
- Be aware of your surroundings at all times
- Be aware that your conversations may not be private or secure
- Do not leave electronic devices unattended
- Clear your internet browser after each use
- Do not wear expensive-looking jewelry and avoid wearing American team sports shirts or baseball caps that might indicate you are an American

## WHEN YOU RETURN

- Review your system access with your information security officer
- Report any unusual circumstances, including contact by foreigners, to the FBI